[520.1007]

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

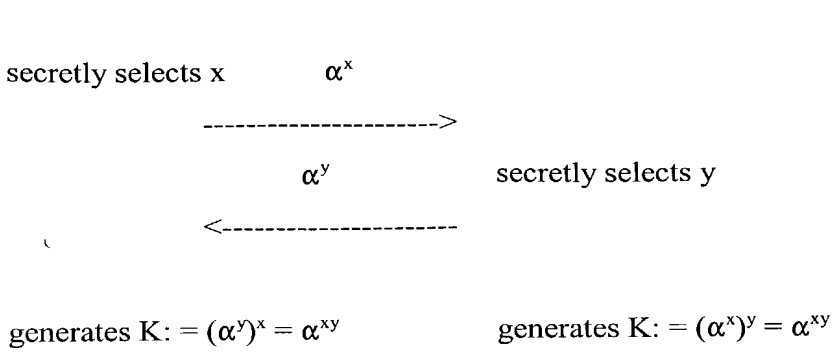
Specification

[0001] The present invention relates to a method for establishing a common key within a group of subscribers according to the definition of the species in the independent claim.

[0002] Encryption methods of varied types belong to state of the art and increasingly have commercial importance. They are used for sending messages over commonly accessible transmission media, but only the owners of a cryptokey being able to read these messages in plain text.

[0003] A known method for establishing a common key over unsecure communication channels is, for example, the method by W. Diffie and W. Hellmann (see DH-Method W. Diffie and M. Hellmann, see New Directions in Cryptography, IEEE Transaction on Information Theory , IT-22(6): 644-654, November 1976).

[0004] The basis of the Diffie Hellmann key exchange (DH-key exchange) is the fact that it is virtually impossible to compute logarithms modulo a large prime number p. In the example depicted below, Alice and Bob make use of this in that they each secretly select a number x or y, respectively, which are smaller than p (and relatively prime to p-1). Then, they (successively or simultaneously) send each other the x^{th} (or y^{th}) power modulo p of a publicly known number α. They are able to compute a common key $K: = \alpha^{xy}$ mod p from the received powers by another exponentiation modulo p with x or y, respectively. An attacker who sees only α^x mod p and α^y mod p cannot compute K therefrom. (The only method for this which is known today would be to initially compute the logarithm, for example, of α^x to base α modulo p, and to subsequently exponentiate α^y therewith.)



Example of the Diffie-Hellmann key exchange

[0005] The difficulty of the DH-key exchange lies in that Alice does not know whether she actually communicates with Bob or with a cheater. In the IPSec-Standards of the Internet Engineering Task Force (IETF RFC 2412: The OAKLEY Key Determination Protocol), this problem is solved by using public key certificates in which the identity of a subscriber is combined with a public key by a trust center. In this manner, the identity of an interlocutor becomes verifiable.

[0006] The DH-key exchange can also be carried out using other mathematical structures, for example, with finite bodies GF (2^n) or elliptical curves. Using these alternatives, it is possible for the performance to be improved. However, this method is only suitable to agree upon a key between two subscribers.

[0007] Several attempts have been made to extend the DH method to three or more subscribers (group DH). An overview of the related art is offered by M. Steiner, G. Tsudik, M. Waidner in Diffie-Hellmann Key Distribution Extended to Group Communication, Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.

[0008] An extension of the DH method to subscribers A, B and C is described, for example,

by the following table (the calculation is in each case mod p):

Subscriber A;B;C	A → B	B → C	C → A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

[0009] Subsequent to carrying out these two rounds, each of the subscribers is able to compute secrete key g^{abc} mod p.

[0010] Known from Burmester, Desmedt, A secure and efficient conference key distribution system, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 is, moreover, a design approach in which two rounds are required for generating the key, it being necessary to send n messages of length p = approx. 1000 bits for n subscribers in the second round.

[0011] Further relevant design approaches are known from M. Burmester and Y. Desmedt, Efficient and secure conference key distribution, Cambridge Workshop on Security Protocols, Springer LNCS 1189, pp 119-129 (1996). However, it is assumed here that secure channels already exist between the subscribers.

[0012] In all of these extensions, at least one of the following problems occurs:

- The subscribers have to be organized in a specific fashion; in the above example, for instance, as a circle, that is, a structure of the subscriber group must previously be known.
- If a central unit is used to coordinate the key agreement, then the subscribers have no influence on the selection of the key with respect to this central unit.
- The number of rounds depends on the number of subscribers.

For the above reasons, these methods are generally difficult to implement and require considerable computational outlay.

[0013] The further development of the DH method to a public key method is known from T. ElGamal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.", IEEE Transactions on Information Theory, July 1985.

[0014] The method according to the present invention has to be suitable for generating a common key within a group of at least three subscribers. The intention is for the method to be designed in such a manner that it stands out over the known methods by a small computational outlay and a small communication requirement (few rounds even in the case of many subscribers). At the same time, however, it is intended to have a comparable security standard as the DH method. The method has to be easy to implement. Information on the structure of the group should not be required for carrying out the method.

[0015] The method according to the present invention which satisfies this problem definition is based on the same mathematical structures as the DH method and has therefore comparable security features. In comparison with the group DH methods proposed heretofore, however, it is considerably more efficient with regard to the computational outlay and communication requirement.

[0016] In the following, the operating principle of the method will be explained in greater detail. The defined subscribers of the method are denoted by T1-Tn and each individual, not specifically named subscriber is denoted by Ti. All other subscribers involved in the method are denoted by Tj except for the respective subscriber Ti. The publicly known components of the method are a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of group G, preferably a number $0 < g < p$ having large multiplicative order. However, it is also possible to use other suitable mathematical structures for group G, for example, the multiplicative group of a finite body or the group of the points of an elliptical curve. In the following, the method will be described on the basis of the group of numbers modulo a prime number p.

[0017] The method is based on four method steps.

In the first method step, a message of the form $Ni = g^{zi} \bmod p$ is generated by each not specifically named subscriber Ti and sent to all other subscribers Tj, zi preferably being a random number from the set {1, ... p-2} selected via a random-number generator.

[0018] In the second method step, each subscriber Ti computes a common transmission key $k^{ij} := (g^{zj})^{zi}$ from received message g^{zj} for each further subscriber Tj, where $i \neq j$. Since $k^{ij} = k^{ij}$ applies, subscribers Ti and Tj now know a common transmission key k^{ij} and can therefore communicate confidentially.

[0019] In the third method step, each subscriber Ti uses transmission key k^{ij} to confidentially send his/her random number zi to the other subscribers Tj, respectively. In the process, the encryption of random number zi with transmission key k^{ij} is carried out using a symmetrical encryption method. This means that, upon completion of the method step, each subscriber Ti knows the encrypted random numbers of all other subscribers Tj in addition to his/her own random number so that the conditions are given for computing a common key k.

[0020] In the fourth method step, common key k is computed according to equation

$k = f(z1, z2, ..., zn)$

at each subscriber Ti, with f being an arbitrary symmetrical function.. In this case, symmetry means that the value of the function remains the same even when arbitrarily exchanging the arguments. Examples of symmetrical functions include

- the multiplication in a (finite) body: $k := z1 \ldots zn$,
- the addition in a (finite) body: $k := z1 + \ldots + zn$,
- the bitwise XOR of zi: $k := z1 \oplus \ldots \oplus zn$,
- the exponentiation of g with zi: $k := g^{z1 \ldots zn}$
- countless further possibilities.

[0021] The transmission of the messages generated in steps 1 and 2 can be carried out both via point-to-point connections and by broadcast or multicast.

[0022] In the following, the method according to the present invention will be explained in greater detail in the light of a concrete example for three subscribers A, B and C. However, the number of subscribers can be extended to an arbitrary number of subscribers.

[0023] In this example, the length of number p is 1024 bits; g has a multiplicative order of at least 2^{160}.

[0024] The method according to the present invention is executed according to the following method steps:

1. Subscriber A sends $Na = g^{za} \bmod p$ to subscribers B and C, subscriber B sends $Nb = g^{zb} \bmod p$ to subscribers A and C, and subscriber C sends $Nc = g^{zc} \bmod p$ to subscribers A and B.
2. Subscriber A computes $kab = Nb^{za} \bmod p$ and $kac = Nc^{za} \bmod p$. Subscribes B and C proceed analogously.
3. Subscriber A sends message Mab = E(kab, za) to subscriber B and message Mac = E(kac, za) to subscriber C. Here, E(k, m) denotes the symmetrical encryption of the data record with algorithm E under transmission key k^{y}. Subscribes B and C proceed analogously.
4. Subscriber A computes common key k according to the function $k = g^{ka \cdot kb \cdot kc}$. Subscribers B and C compute common key k analogously.

[0025] The method described above makes do with the minimum number of two rounds between subscribers A, B and C. The number of rounds required for carrying out the method according to the present invention remains limited to two rounds even with an arbitrary number of subscribers T1-Tn .

[0026] A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 or b and c are executed only by subscriber T1. In fourth method step d, all subscribers T1-Tn involved in the method compute common key k according to the relation $k: = h(z1, g^{z2}, ..., g^{zn})$, it being required for (x1, x2, ..., xn) to be a function which is

symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1 \cdot z1} \cdot g^{z2 \cdot z1} \ldots \; g^{zn\, z1}.$$

[0027] The method according to the present invention can be advantageously used to generate a cryptographic key for a group of a several or at least three subscribers.

[0028] List of Reference Symbols

T1-Tn	subscribers 1 through n
Ti	undefined subscriber of T1-Tn
Tj	undefined subscriber of T1-Tn, different from Ti.
N	message
Ni	message of an undefined subscriber Ti
Mab	message of subscriber A to subscriber B
G	publicly known mathematical group
g	element of group G
p	large prime number
z	random number from the set (1,...p-2) selected via a random-number generator
k^{ij}; k^{1j}	common transmission key
k	common key
E(,)	algorithm
m	data record
f(x1,x2,...,xn)	function symmetrical in x1,x2,...,xn.
h(x1,x2,...,xn)	function symmetrical in arguments x2,...,xn.
A; B; C	designation of the subscribers in the exemplary embodiment